(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
27 September 2001 (27.09.2001)

PCT

(10) International Publication Number
WO 01/72030 A2

(51) International Patent Classification[7]: H04N 1/32

(21) International Application Number: PCT/EP01/02915

(22) International Filing Date: 15 March 2001 (15.03.2001)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
09/531,700 20 March 2000 (20.03.2000) US

(71) Applicant: KONINKLIJKE PHILIPS ELECTRONICS N.V. [NL/NL]; Groenewoudseweg 1, NL-5621 BA Eindhoven (NL).

(72) Inventor: KRISHNAMACHARI, Santhana; Prof. Holstlaan 6, NL-5656 AA Eindhoven (NL).

(74) Agent: SCHMITZ, Herman, J., R.; Internationaal Octrooibureau B.V., Prof Holstlaan 6, NL-5656 AA Eindhoven (NL).

(81) Designated States *(national)*: CN, JP, KR.

(84) Designated States *(regional)*: European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR).

Published:
— *without international search report and to be republished upon receipt of that report*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

WO 01/72030 A2

(54) Title: HIERARCHICAL AUTHENTICATION SYSTEM FOR IMAGES AND VIDEO

(57) Abstract: A method and system for creating authentication signatures for digital images and video frames is provided. The method and system involves partitioning the image into multiple blocks, comparing characteristics from each block and generating data bits based on the comparison. Each block is then broken up into additional blocks and those blocks are compared to create additional signature bits which are combined with the signature sets from the first set of blocks. Each of these new smaller blocks can be further broken up and the procedure can be repeated to provide an authentication signature of desired length.

Hierarchical authentication system for images and video

BACKGROUND OF THE INVENTION

The invention relates generally to authentication systems and methods for digital images and more particularly to improved methods, systems and signals for authenticating digital images.

The use of digital images and videos by both consumers and professionals is pervasive. Accordingly, it has become important to provide a system and method for authenticating digital images and videos to insure that they have not been tampered with. As an example, an authentication system could insure that someone has not replaced a person's face with that of another on a digital picture or series of video frames.

Authentication systems are known which extract a short signature from images (or video frames) which can be either inserted into the image signal or stored separately. The owner of the original content can use the signature to verify whether the content has been modified or users can confirm that they are receiving authentic digital images.

Conventional content-based image authentication systems typically define an image into many blocks and extract characteristics about the blocks. For example, the image can be broken up into 16 x 16 blocks as in FIG. 1 or some other number of blocks, and some characteristic about the block, such as average luminance or chrominance values with respect to R, G, B or gray values. The characteristics of adjacent pairs of blocks are commonly compared and a signature is extracted based on this comparison. For example, if the average luminance value for the red component of a first block 110 of an image 100 is greater than or equal to that of a second block 120, a one bit will be generated. Otherwise, a zero bit will be generated. The process is repeated with successive blocks until a binary signature of ones and zeros is compiled.

A disadvantage to this method is that because pairs of blocks each contribute a bit to the signature, it is possible to change the pair of blocks without affecting the signature by maintaining the difference or similarity of the compared characteristic of each block. It can be possible to reverse engineer the signature and then alter the image in such a manner to generate an identical signature and thus frustrate the authentication mechanism.

The following references discuss processing video signals, coding image blocks and authentication algorithms for digital images, the contents of which are incorporated herein by reference: WO 93/11502, US 4,254,400, US 5,351,095, US 5,520,290 and US 5,870,471.

Techniques for performing pair-wise block comparisons in a non-hierarchical technique are discussed in "Generating robust digital signature for image/video authentication", C.Y. Lin and S.F. Chang, in Proceedings of Multimedia and Security Workshop at A.C.M. Multimedia, September 1998. Inserting and/or hiding a signature in an image signal is discussed in "Secure spread spectrum water marking for images, audio and video," I. Cox, et al., in IEEE Int'l. Conf. on Image Processing, Vol. 3, pp. 243-246 (1996). The contents of these references are incorporated herein by reference.

Accordingly, it is desirable to provide an improved method and system for authenticating digital images which overcomes drawbacks of conventional methods and systems.

SUMMARY OF THE INVENTION

Generally speaking, in accordance with the invention, a method and system for creating authentication signatures for digital images is provided. The method and system involves partitioning the image into multiple blocks, comparing characteristics from each block and generating signature data bits based on the comparison. Each block can then be broken up into additional blocks and those blocks can be compared to create additional sets of signature bits which can be combined with the signature bits from the first set of blocks. Each or a portion of these new smaller blocks can be further broken up and the procedure can be repeated to provide an authentication signature of desired length by combining all or parts of the signature segments.

Accordingly, it is an object of the invention to provide an improved method and system for authenticating digital images and video.

Another object of the invention is to provide a method of creating an authentication signature for a digital image which is difficult to duplicate if the image is altered.

Another object of the invention is to provide an improved system for creating, storing and using authentication signatures for digital images which are difficult to duplicate if the original image is altered.

The invention accordingly comprises the several steps and relation of one or more of such steps with respect to each of the others and the product, system, signal and media adapted to effect or resulting from such steps, or as is exemplified in the following detailed description and drawings and the scope of the invention will be indicated in the claims.

BRIEF DESCRIPTION OF THE DRAWINGS

For a fuller understanding of the invention, reference is had to the following description, taken in connection with the accompanying drawings, in which:

FIG. 1 represents a digital image divided into sixteen blocks;

FIG. 2A represents the partition of an image into four blocks at scale zero;

FIG. 2B shows each of the blocks of FIG. 2A broken down into four sub-blocks at scale one;

FIG. 3 is a flow chart of an authentication method in accordance with an embodiment of the invention;

FIG. 4 is a flow chart of an authentication method in accordance with another embodiment of the invention; and

FIG. 5 is a flow chart of an authentication method in accordance with an embodiment of the invention.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

Authentication algorithms for digital data should be difficult to reverse engineer and should insure that it is difficult, if not impossible to alter the image without changing the correspondence between the authentication signature and the image itself. The authentication is preferably performed in a content-based fashion and small, non-malicious changes in the image such as brightening or subjecting the image to various coding or compression algorithms, such as a lossy JPEG-like compression should be allowed. As used herein, the term image will also be used to refer to video frames.

Authentication methods and systems in accordance with the invention use a hierarchical technique, where the image is partitioned into blocks of a selected number of pixels at a first-level or scale (scale 0) and then each or a portion of the blocks are further partitioned into sub-blocks in successive scales. At each scale, the properties or characteristics of blocks (or sub-blocks) are compared to obtain a signature for that scale, and all or part of the signatures for each scale are combined. As the individual blocks are broken

down into successive scales of greater detail, the authentication signature generated at each scale can be added onto or otherwise combined with the signature generated from previous scale levels to provide a more robust signature which is more difficult to reverse engineer and evade, compared to conventional mono-scale techniques.

Referring to FIG. 2A, as a non-limiting illustration of a technique in accordance with preferred embodiments of the invention, the image (not shown) has been partitioned into four non-overlapping blocks at scale zero. These blocks are identified as A, B, C and D. The blocks together completely cover the entire image. It is also possible, in accordance with preferred embodiments of the invention, to use overlapping blocks or blocks which cover only a portion of the image, such as when authentication is only desired for a particular section of an image. Partitioning only a portion of the image can simplify the procedure if characteristic information will only be located at a certain location of the image.

A characteristic value is extracted from each block. This characteristic can be a luminance or chrominance characteristics, and the value can be the average luminance of the R (red) value (for example) over the entire block. Other values for the characteristics, such as the standard deviation of the characteristic of the block or some other characteristic value such as DCT coefficient and the like can be used. The computed characteristic values can be identified as $f(A)$, $f(B)$, $f(C)$ and $f(D)$ where f is the function used to compute the desired characteristic value.

The computed characteristic values of the four blocks can then be compared as follows. The $f(\ )$ values can be arranged in an ascending, descending or other predefined order. Because there are four blocks, there are twenty-four possible combinations of the ordering. (e.g., ABCD, ABDC, ADBC...). A five-bit binary number can be used to represent each combination in the ordering, i.e., ABCD could be assigned 00001 and CBDA might be assigned 10010. A five-bit binary number can represent 32 different combinations. The remaining eight combinations can be used for the instances where the values of some of the $f(\ )$ characteristics are equal. For example, if the four values are all equal, e.g., if the average green level of each block is identical, then a particular 5-bit number such as 11111 can be used to specify that particular combination. Thus, a 5-bit number is obtained at scale 0 (level 1) to form a part of the authentication signature.

Although four blocks are shown in this embodiment of the invention, different numbers of blocks and sub-blocks can be used in alternate embodiments of the invention. Also, the number of sub-blocks, to which a block (or sub-block) is divided need not be identical to the number of blocks or sub-blocks of a higher scale. If the number of blocks is

greater than four, then the number of bits used to represent all of the combination will be greater than five.

Referring to FIG. 2B, each of the four blocks from scale 0 (FIG. 2A) are partitioned into four non-overlapping sub-blocks designated AA, AB and so forth. (As noted above, each of the blocks of FIG. 2A could have been divided into two sub-blocks , nine sub-blocks and so forth.) The partitioning of the image as shown in FIG. 2B represents scale 1 in the hierarchical decomposition. The characteristic values of each of blocks AA, AB, AC and AD are computed as discussed above and a 5-bit binary number is obtained for the four groups of sub-blocks of the scale 0 blocks. In alternate embodiments of the invention, different characteristics from those used at scale 0 can be used in each of the additional scales.

After the characteristic values of sub-blocks AA, AB, AC and AD are computed, a 5-bit binary number is obtained. The same process is repeated for the three other sets of sub-blocks at scale 1, resulting in four 5-bit numbers or 20 bits. These 20 bits are combined with the first 5-bit number and the process can be repeated successively for additional sets of sub-blocks at higher scales. The bits obtained from successive scales are concatenated to obtain a signature. For example, if four scales are used, then 5-bits are obtained from scale 0, 20-bits from scale 1, 80-bits from scale 2, and 320-bits from scale 3. All of these bits are concatenated to form a 425-bit level 4 authentication signature.

In alternate embodiments of the invention, the authentication signature can be obtained for a first color band and then similar signatures can be obtained for the additional color bands. The number of scales used would depend on the size of the image and the desired length of the signature.

The signature can be stored separately or sent with the image signal and transmitted with the signal or stored on a floppy disk, CD, DVD, video tape and the like.

A flow chart 500 corresponding to an authentication method in accordance with preferred embodiments of the invention is shown generally in FIG. 5. In step 510, image data 501 is divided into blocks. In step 520, values corresponding to characteristics of each block are calculated. In step 530, the blocks are ordered based on the values and in step 540, a first-level binary code corresponding to the order of the blocks is assigned. In step 550, each block from the first-level (scale 0) is subdivided into sub-blocks. In step 560, values for each sub-block are calculated and in step 570, the sub-blocks are ordered based on these values. In step 580, sets of binary codes corresponding to the ordered sets of sub-blocks are generated and in step 590, the binary code is combined with the first-level binary

code. In step 600, the process can be repeated and additional levels (scales) of authentication signature binary code can be developed.

Non-limiting uses of the signature obtained in accordance with preferred embodiments of the invention are illustrated in FIGS. 3 and 4.

Referring to FIG. 3, a data processor can be used to extract the authentication signature from image data using hierarchical algorithms discussed above in step 310. In step 320 the signature of the image or video frame can be inserted into or added to the signal representing the image. In step 330 the image together with the inserted signature can be transmitted to an image receiver.

In step 340, the authentication signature can be extracted from the image data using the hierarchical algorithm. In step 350, the inserted (hidden) signature from the image is extracted.

In step 360, the signature generated from the transmitted signal is compared to the signature inserted with the image. If they match, authentication is acknowledged in step 370. If they do not match, authentication failure is indicated in step 380.

Referring to FIG. 4, a method of authentication is illustrated where the signature is not inserted into the image signal. In step 410 the authentication signature of an image or video frame is extracted using a hierarchical algorithm in accordance with the invention. In step 420, this signature is stored at a secure location. When verification is desired, in step 430, the authentication signature is extracted from the image or video frame using the hierarchical algorithm. In step 440, the signature is compared to that stored during step 420 and if they match, authentication is acknowledged in step 450. Otherwise, authentication failure is noted in step 460.

CLAIMS:

1. A method of creating an authentication signature corresponding to an image (100), comprising:

partitioning at least a portion of an image (100) into a selected number of first-level blocks of image information (510);

determining a first-level block value corresponding to a characteristic of the portion of the image contained in each first-level block (520);

processing the first-level block values for the first-level blocks (530) and generating a first-level signature segment based on the first-level block values as a result of such processing (540);

subdividing each first-level block into a selected number of second-level sub-blocks (550);

determining a second-level sub-block value corresponding to a characteristic of the portion of the image contained in each second-level sub-block (560);

processing the second-level block values for the second-level sub-blocks (570) and generating a second-level signature segment based on the second-level block values as a result of such processing (580); and

combining at least a portion of the second-level signature segment with at least a portion of the first-level signature segment (590).

2. The method of claim 1, wherein the characteristic of the image is based on chrominance or luminance values for the blocks or sub-blocks.

3. The method of claim 1, wherein the first-level signature segment is generated by ordering the blocks based on the first-level block value for each block and generating a binary code corresponding to the order of the blocks.

4. The method of claim 3, wherein the second-level signature segment is generated by ordering the sub-blocks based on the second-level value for each sub-block and generating binary codes corresponding to the ordered sub-blocks and the binary codes

corresponding to the second-level signature segment are combined with the binary code corresponding to the first-level signature segment (590).

5. The method of claim 4, wherein the order of the four first-level blocks (A, B, C, D) are assigned a binary code.

6. The method of claim 5, wherein the second-level signature is generated by ordering the sub-blocks (AA, AB, AC, AD) based on the second-level sub-block values and assigning binary codes to groups of four sub-blocks (AA, AB, AC, AD).

7. The method of claim 6, wherein the blocks are ordered in ascending or descending order of the first-level block values and second-level block values.

8. The method of claim 7, wherein selected binary codes for the signature segment are assigned when the first-level block values or second-level block values of two or more blocks or sub-blocks are equal.

9. The method of claim 1, wherein at least a portion of the second-level sub-blocks are subdivided into a selected number of third-level sub-blocks, third level signature segments are generated from the third-level sub-blocks and the third-level signature segments are combined with the first and second-level signature segments (600).

10. A method of creating an authentication signature corresponding to an image (100), comprising:

partitioning at least a portion of an image into a selected number of first-level blocks of image information (510);

determining a first-level block value corresponding to a characteristic of the portion of the image contained in each first-level block (520);

ordering the blocks based on the first-level block values for the first-level blocks (530) and generating a first-level signature segment corresponding to the resulting order (540);

subdividing each first-level block into a selected number of second-level sub-blocks (550);

determining a second-level sub-block value corresponding to a characteristic of the portion of the image contained in each second-level sub-block (560);

ordering the sub-blocks based on the second-level block values (570) and generating a second-level signature segment corresponding to the order of the sub-blocks (580); and

combining the second-level signature segment with the first-level signature segment (590).

11. A system for providing an authentication signature corresponding to a digital image, comprising:

a data processor constructed to receive data representing an image (501); partition at least a portion of the image into a selected number of first-level blocks of image information (510); determine first-level block values corresponding to a characteristic of the portion of the image contained in each first-level blocks (520); process the first-level block values for the first-level blocks (530); generate a first-level signature segment as a result of such processing (540); subdivide each first-level block into a selected number of second-level sub-blocks (550); determine a second-level sub-block value corresponding to a characteristic of the portion of the image contained in each second-level sub-block (560); and process the second-level block values for the second-level sub-blocks (570) and generate a second-level signature segment as a result of such processing (580).

12. The system of claim 11, wherein the data processor is constructed to determine the first level block value based on chrominance or luminance values for the blocks or sub-blocks.

13. The system of claim 11, wherein the data processor is constructed to subdivide at least some of the second-level sub-blocks into a selected number of third-level sub-blocks and generate signature segments based on the third-level sub-blocks (600).

14. A system for creating an authentication signature corresponding to an image, comprising:

a data processor constructed to receive data representing an image (501); partition at least a portion of an image into a selected number of first-level blocks of image information (510); determine a first-level block value corresponding to a characteristic of the

portion of the image contained in each first-level block (520); order the blocks based on the first-level block values for the first-level blocks (530); generate a first-level signature segment corresponding to the resulting order (540); subdivide each first-level block into a selected number of second-level sub-blocks (550); determine a second-level sub-block value corresponding to a characteristic of the portion of the image contained in each second-level sub-block (560); order the sub-blocks based on the second-level block values (570); generate a second-level signature segment corresponding to the order of the sub-blocks (580); and combine the second-level signature segment with the first-level signature segment (590).

15. A data storage medium containing data representing an image and a signature corresponding to the image generated by the steps comprized partitioning at least a portion of an image into a selected number of first-level blocks of image information (510); determining a first-level block value corresponding to a characteristic of the portion of the image contained in each first-level block (520); processing the first-level block values for the first-level blocks (530) and generating a first-level signature segment based on the first-level block values as a result of such processing (540); subdividing each first-level block into a selected number of second-level sub-blocks (550); determining a second-level sub-block value corresponding to a characteristic of the portion of the image contained in each second-level sub-block (560); processing the second-level block values for the second-level sub-blocks (570); and generating a second-level signature segment based on the second-level block values as a result of such processing (580).

16. An image authentication system, comprising:

providing a first image (100);

generating an authentication signature (410) by a first method comprising partitioning at least a portion of an image into a selected number of first-level blocks of image information (510); determining a first-level block value corresponding processing the first-level block values for the first-level blocks (530) and generating a first-level signature segment based on the first-level block values as a result of such processing (540);

subdividing each first-level block into a selected number of second-level sub-blocks (550); determining a second-level sub-block value corresponding to a characteristic of the portion of the image contained in each second-level sub-block (560); processing the second-level block values for the second-level sub-blocks (570) and generating a second-level signature segment

based on the second-level block values (580) as a result of such processing; and combining the second-level signature segment with the first-level signature segment (590);

providing a second image which may be identical to the first image;

generating a second signature for the second image by the first method (430); and

comparing the first signature to the second signature (440).

17. A method of creating an authentication signature for an image, comprising:

dividing an image into a first level portion or portions (510) and generating a signature segment based on that portion or portions of the image (540); and

subdividing the first level portion or portions of the image into second level sub-portions (500) and generating signature segments based on the subdivisions (580).

18. The method of claim 17, including further subdividing portions of the image and generating additional signature segments based on said further subdivisions (600).

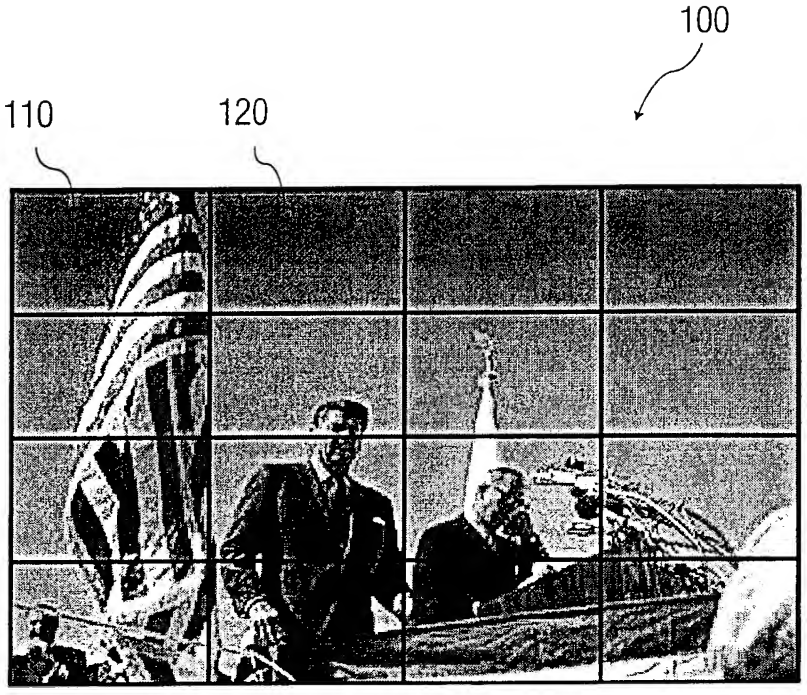

FIG. 1

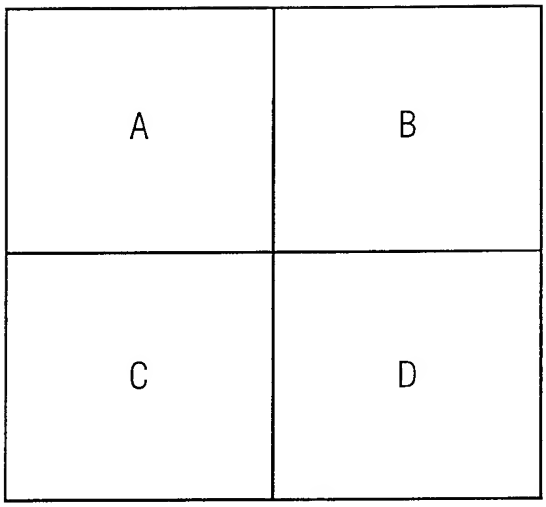

FIG. 2A

AA	AB	BA	BB
AC	AD	BC	BD
CA	CB	DA	DB
CC	CD	DC	DD

FIG. 2B

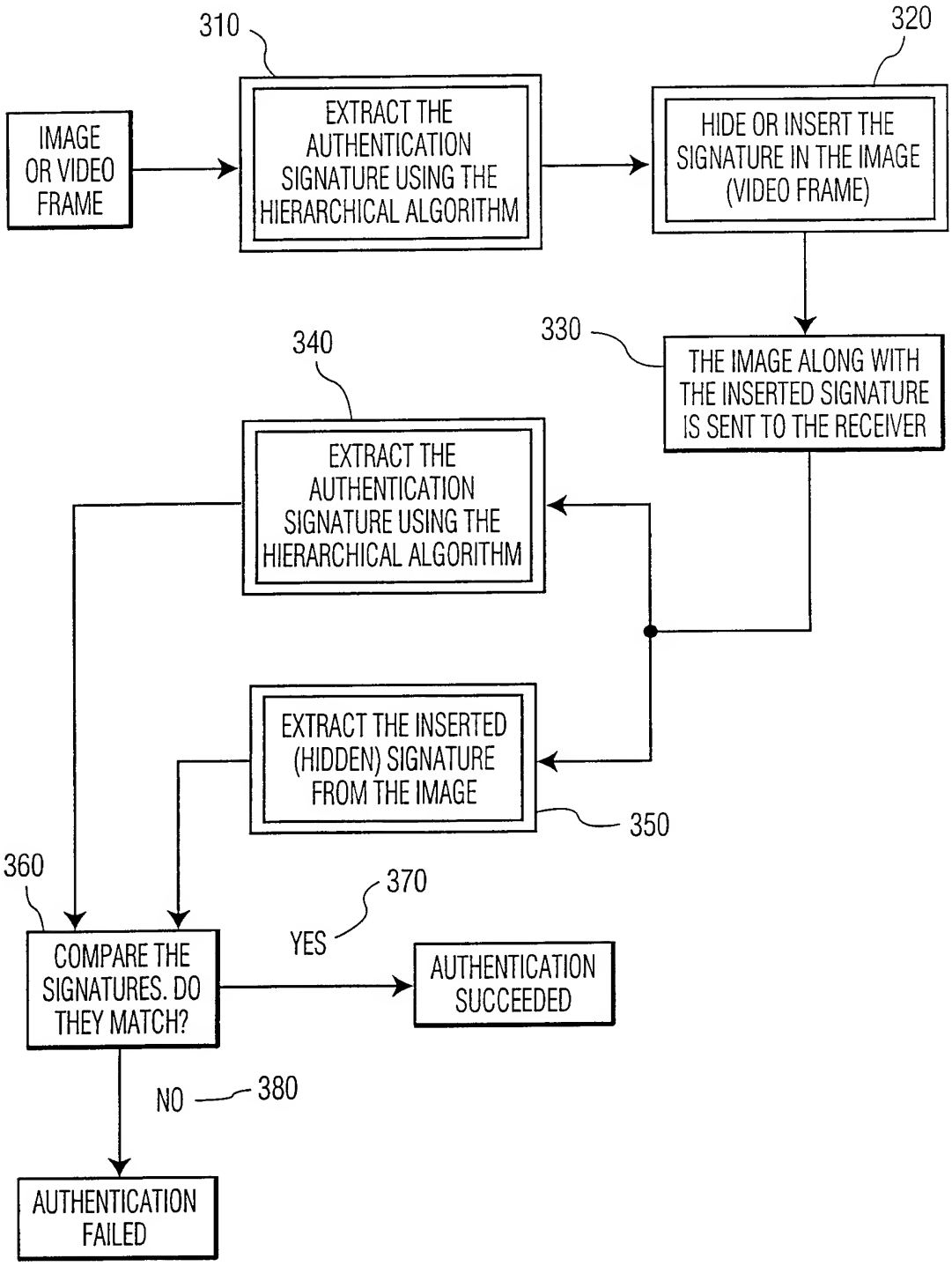
310
320
IMAGE OR VIDEO FRAME
EXTRACT THE AUTHENTICATION SIGNATURE USING THE HIERARCHICAL ALGORITHM
HIDE OR INSERT THE SIGNATURE IN THE IMAGE (VIDEO FRAME)
330
THE IMAGE ALONG WITH THE INSERTED SIGNATURE IS SENT TO THE RECEIVER
340
EXTRACT THE AUTHENTICATION SIGNATURE USING THE HIERARCHICAL ALGORITHM
EXTRACT THE INSERTED (HIDDEN) SIGNATURE FROM THE IMAGE
350
360
370
YES
COMPARE THE SIGNATURES. DO THEY MATCH?
AUTHENTICATION SUCCEEDED
NO
380
AUTHENTICATION FAILED

FIG. 3

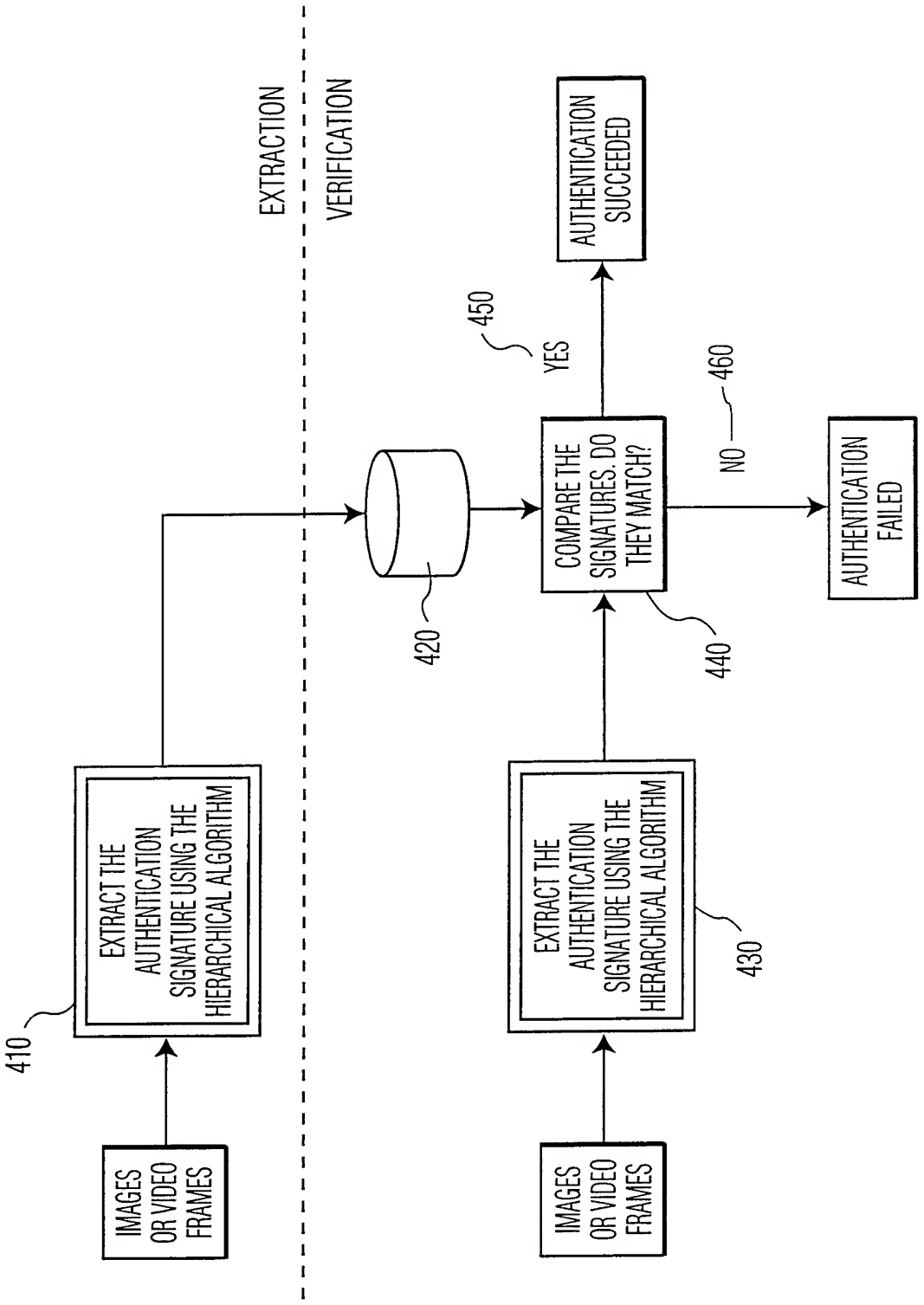
EXTRACTION
VERIFICATION
IMAGES OR VIDEO FRAMES
EXTRACT THE AUTHENTICATION SIGNATURE USING THE HIERARCHICAL ALGORITHM
410
420
IMAGES OR VIDEO FRAMES
EXTRACT THE AUTHENTICATION SIGNATURE USING THE HIERARCHICAL ALGORITHM
430
COMPARE THE SIGNATURES. DO THEY MATCH?
440
450
YES
AUTHENTICATION SUCCEEDED
460
NO
AUTHENTICATION FAILED

FIG. 4

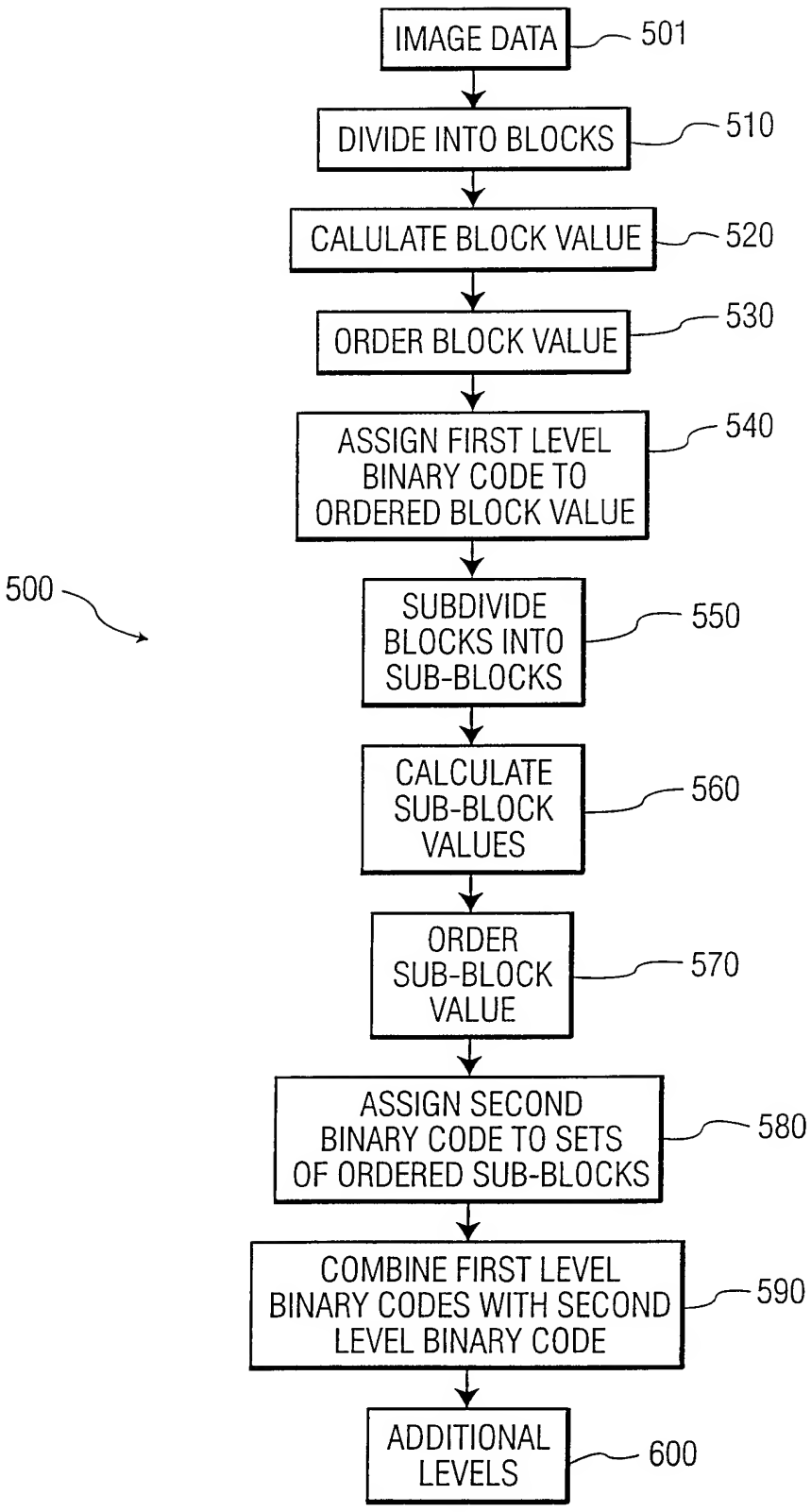
IMAGE DATA
501
DIVIDE INTO BLOCKS
510
CALULATE BLOCK VALUE
520
ORDER BLOCK VALUE
530
ASSIGN FIRST LEVEL BINARY CODE TO ORDERED BLOCK VALUE
540
500
SUBDIVIDE BLOCKS INTO SUB-BLOCKS
550
CALCULATE SUB-BLOCK VALUES
560
ORDER SUB-BLOCK VALUE
570
ASSIGN SECOND BINARY CODE TO SETS OF ORDERED SUB-BLOCKS
580
COMBINE FIRST LEVEL BINARY CODES WITH SECOND LEVEL BINARY CODE
590
ADDITIONAL LEVELS
600

FIG. 5